Before we begin...

- Elasticsearch aggregations are used for all Kibana visualizations
- You *should* be familiar with the basics of aggregations
  - ... but if not, here is a quick introduction 🙂
  - If you *are* familiar with them, you can skip to the next lecture 🚀

Elasticsearch aggregations

- Aggregations group documents together
  - The purpose is to retrieve analytical information from them
- Categories relevant to Kibana
  - Bucket aggregations
  - Metric aggregations
  - Pipeline aggregations

Bucket aggregations

- Creates *buckets* (groups) of documents
- A bucket is a set of documents matching a criterion
    - A document “falls into” the bucket if it matches the criterion
- E.g. the `terms` aggregation that creates a bucket for each unique field value
- We cannot access the actual documents within buckets
    - We can run *metric aggregations* on them, though

Metric aggregations

- Compute metrics over buckets, using document fields
- E.g. using the `sum` aggregation to get order totals for each bucket
- Can be applied at all levels
- Other metric aggregations; `avg`, `min`, `max`, `cardinality`, etc.

Pipeline aggregations

- Advanced, so we won't go into detail
- Operate on other aggregations, *not* buckets
- E.g. use the result of a `sum` aggregation in calculations